ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

# ICS-CERT ADVISORY

## ICSA-13-077-01A—SCHNEIDER ELECTRIC PLCS MULTIPLE VULNERABILITIES

UPDATE A

March 20, 2013

## OVERVIEW

**--------- Begin Update A Part 1 of 1 --------**

This updated advisory is a follow-up to the original advisory titled ICSA-13-077-01—Schneider Electric PLCS Multiple Vulnerabilities that was published March 18, 2013, on the ICS-CERT Web page. It is also a follow-up to the updated alert titled ICS-ALERT-13-016-01A—Schneider Electric Multiple Vulnerabilities[a] that was published March 5, 2013, on the ICS-CERT Web page. This advisory corrects and expands on the details in the specified alert.

This updated advisory provides mitigation details for multiple vulnerabilities that affect Schneider Electric Modicon, Premium, and Quantum PLC modules.

Independent researcher Arthur Gervais has identified two vulnerabilities in the common Ethernet modules used across a broad range of Schneider Electric's PLC products. These vulnerabilities were disclosed at the 2013 Digital Bond SCADA Security Scientific Symposium (S4) conference in January 2013. An improper authentication vulnerability and cross-site request forgery vulnerability have been validated by Schneider Electric. Schneider Electric has released

a. ICS-ALERT-13-016-01A, http://ics-cert.us-cert.gov/pdf/ICS-ALERT-13-016-01A.pdf, last accessed March 20, 2013.

mitigations for these vulnerabilities[b] but does not plan to issue patches because of their complex nature. Schneider Electric says that fixing these vulnerabilities would require significant changes to existing protocols and make any customer solutions currently using these features incompatible.

These vulnerabilities could be exploited remotely.

Additional issues reported by the researcher have also been investigated by the vendor.

The vendor and researcher disagree on whether Magelis XBT HMI issue is a valid vulnerability. The Magelis XBT HMI panels have a security mode where a password is required to enable remote configuration uploads. After this mode is initially enabled, a factory default password is provided. The user is not prompted or required to supply a new password, although this capability is provided. Once the user supplies a new password, the factory default password is no longer valid. This does not fit the definition of a hard-coded password, because it can be changed. Users should be aware of the potential for configuration errors that can lead to significant security issues.

The reported Resource Exhaustion issue affecting the M340 PLC family could not be duplicated by the vendor given the information supplied by the researcher. Software versions or specific configuration differences could account for the inability of the vendor to duplicate the results. In Schneider Electric's testing on this issue, the communications module does in fact stop communicating when the connection limit is exceeded, but the PLC continues its control functions and its operation is unaffected. After the connection limit is exceeded, the communications module performs a soft reset. An attacker could not remotely exploit this observed behavior to deny PLC control functions. Although the researcher-reported behavior could not be duplicated, the vendor could not go any further with addressing it without more specific detailed information.

The remainder of this advisory addresses the two vulnerabilities that the vendor did confirm.

**--------- End Update A Part 1 of 1 --------**

b. Schneider Electric Disclosure http://www.schneider-electric.com/download/ww/en/details/35081317-Vulnerability-Disclosure-for-Quantum-Premium-and-M340/, last accessed March 18, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

## AFFECTED PRODUCTS

The following Schneider Electric products are affected:

- Modicon M340 PLC modules,
- Quantum PLC modules, and
- Premium PLC modules.

## IMPACT

A malicious attacker may remotely halt, reset, or change settings for PLC modules by exploiting these vulnerabilities. This could affect products deployed in the critical manufacturing, energy, water, agriculture and food, dams, transportation, postal, nuclear, government facilities, and defense industrial sectors worldwide.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

## BACKGROUND

Schneider Electric is a Europe-based company that maintains offices in 190 countries worldwide. Their PLC products are used in a wide variety of automation and control applications across all industrial, infrastructure, and building sectors.

The affected PLC products, Modicon M340, Quantum, and Premium lines are PLC devices that are used in the United States, China, Russia, and India, and throughout the rest of the world. Primary application areas for these PLCs are in control and monitoring applications across the critical manufacturing, energy, water, agriculture and food, dams, transportation, postal, nuclear, government facilities, and defense industrial sectors.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

## VULNERABILITY CHARACTERIZATION

### VULNERABILITY OVERVIEW

#### IMPROPER AUTHENTICATION[c]

Products supporting the Factory Cast feature, including the Modicon M340, Quantum, and Premium PLC ranges, allow users to send Modbus messages embedded in HTTP POST requests using SOAP messages. Modbus commands sent to the PLC via this mechanism are not authenticated. These messages can result in unintended consequences such as halting operation or modification of I/O data to and from the PLC.

CVE-2013-0664[d] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[e]

#### CROSS-SITE REQUEST FORGERY[f]

The affected devices incorporate a Web server interface that receives requests from clients without a mechanism for verifying that it was intentionally sent. It is possible for an attacker to trick a client into making an unintentional request to the Web server, which will be treated as an authentic request. Valid commands could be sent to the PLC via specially crafted HTTP requests.

CVE-2013-0663[g] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:S/C:C/I:C/A:C).[h]

c. CWE-287, http://cwe.mitre.org/data/definitions/287.html, CWE-287: Improper Authentication, Web site last accessed March 20, 2013.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0664 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C) , Web site last visited March 20, 2013.

f. CWE-352, http://cwe.mitre.org/data/definitions/352.html, CWE-352: Cross-Site Request Forgery, Web site last March 20, 2013.

g. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0663 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

h. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:S/C:C/I:C/A:C) , Web site last visited March 20, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

## VULNERABILITY DETAILS

### EXPLOITABILITY

These vulnerabilities could be exploited remotely.

### EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

### DIFFICULTY

An attacker with a low to medium skill would be able to exploit these vulnerabilities.

## MITIGATION

Schneider Electric has not issued a patch or software update to mitigate these vulnerabilities, but has issued a vulnerability disclosure notification[i] that contains the following recommended mitigations for both vulnerabilities:

- Do not connect the affected PLC modules to an untrusted network.
- If such a connection is required, block all HTTP access to the module from untrusted IP addresses using a firewall, and only allow HTTP connections from known IP addresses from secured workstations.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth

i. Schneider Electric Disclosure http://www.schneider-electric.com/download/ww/en/details/35081317-Vulnerability-Disclosure-for-Quantum-Premium-and-M340/, last accessed March 20, 2013.



Strategies.[j] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies,[k] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

## ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

## DOCUMENT FAQ

**What is an ICS-CERT Advisory?** An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

**When is vulnerability attribution provided to researchers?** Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

j. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed March 20, 2013.
k. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed March 20, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

**I see that this document is labeled as TLP = WHITE. May I distribute this to other people?**
According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[l,m] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.

**TLP =** WHITE: Unlimited

l. Traffic Light Protocol—International CIIP Directory, Issue 21, September 2009.
m. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed March 20, 2013.